INTERNATIONAL JOURNAL OF TECHNOLOGICAL EXPLORATION AND LEARNING (IJTEL)
www.ijtel.org

Advanced File Sharing in Peer to Peer Systems

P.S.G.Aruna Sri
Department of Electronics & Computer Engineering,
KL University,
Vijayawada, Andhra Pradesh

T.Sainath, K.Rahul Kumar, B.Divya, M.Vijaya Durga
Department of Electronics & Computer Engineering
KL University,
Vijayawada, Andhra Pradesh

Abstract—**File Sharing in Peer-to-Peer Networks are a tedious process. For a particular peer to access the files owned by other peer it has to recognize the details of the desired file. Whenever a peer requires a file, it transmits a request to the other peer, which processes the request and demands a decision whether to send the file or not. There is no option for a peer to share its files with other peers. Here in this implementation a option for recommendation is offered. Practicing this, a peer can recommend a file to another peer. The peer which receives the recommendation decides whether it needs the file or not and takes action respectively.**

Keywords- Ethernet (ieee 802.3); Networking; Peer to Peer systems; File Sharing; Connectivity.

I. INTRODUCTION

Networking is the word basically relating to computers and their connectivity. It is very often used in the world of computers and their use in different connections. The term networking implies the link between two or more computers and their devices, with the vital purpose of sharing the data stored in the computers, with each other. The networks between the computing devices are very common these days due to the launch of various hardware and computer software which aid in making the activity much more convenient to build and use.

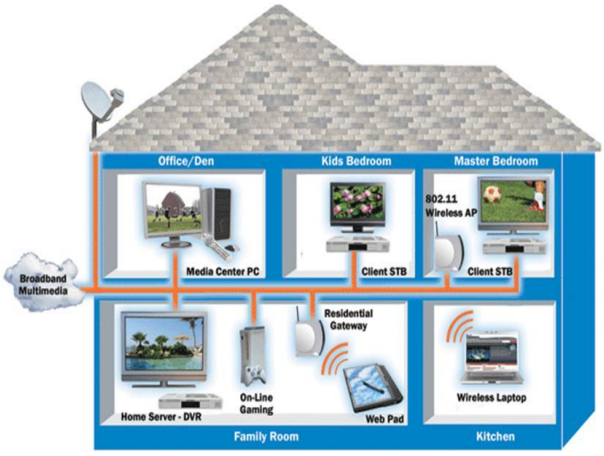


Figure 1. Structure of Networking between the different computers

A. General Network Techniques

When computers communicate on a network, they send out data packets without knowing if anyone is listening. Computers in a network all have a connection to the network and that is called to be connected to a network bus. What one computer sends out will reach all the other computers on the local network. For the different computers to be able to distinguish between each other, every computer has a unique ID called MAC-address (Media Access Control Address). This address is not only unique on your network but unique for all devices that can be hooked up to a network. The MAC-address is tied to the hardware and has nothing to do with IP-addresses. Since all computers on the network receives everything that is sent out from all other computers the MAC-addresses is primarily used by the computers to filter out incoming network traffic that is addressed to the individual computer. When a computer communicates with another computer on the network, it sends out both the other computers MAC-address and the MAC-address of its own. In that way the receiving computer will not only recognize that this packet is for me but also, who sent this data packet so a return response can be sent to the sender.

B. On an Ethernet network

As described here, all computers hear all network traffic since they are connected to the same bus. This network structure is called multi- drop.

One problem with this network structure is that when you have, let say ten (10) computers on a network and they communicate frequently and due to that they sends out there data packets randomly, collisions occur when two or more computers sends data at the same time. When that happens data gets corrupted and has to be resent. On a network that is heavy loaded even the resent packets collide with other packets and have to be resent again. In reality this soon becomes a bandwidth problem. If several computers communicate with each other at high speed they may not be able to utilize more than 25% of the total network bandwidth since the rest of the bandwidth is used for resending previously corrupted packets. The way to minimize this problem is to use network switches.

II. NETWORKING TYPES

Organizations of different structures, sizes, and budgets need different types of networks. Networks can be divided into one of two categories

A. Peer-to-Peer Network

A peer-to-peer network has no dedicated servers; instead, a number of workstations are connected together for the purpose of sharing information or devices. Peer-to-

peer networks are designed to satisfy the networking needs of home networks or of small companies that do not want to spend a lot of money on a dedicated server but still want to have the capability to share information or devices like in school, college, cyber café.

B. *Server-Based Networks*

In server-based network data files that will be used by all of the users are stored on the one server. With a server-based network, the network server stores a list of users who may use network resources and usually holds the resources as well. This will help by giving you a central point to set up permissions on the data files, and it will give you a central point from which to back up all of the data in case data loss should occur.

III. EXISTING SYSTEM FOR FILE SHARING

There are many existing peer-to-peer applications in the present software ecosystem. These applications offer an exchange of data between the peers existing in the network. Such Applications maintain a centralized server for storing this data. Whenever a peer gets to know about a file it might need from another user, it sends a request to the owner peer. This Request is reviewed by the concerning peer and a deserving action is taken. The file requested may or may not be sent to the other peer.

Observing all this, one can say that a particular data can be accessed only if its existence is known. In some cases even if this is known, that file may not be accessed because of ignorance of its other details. This is a hindrance in ensuing effective data sharing.

Disadvantages

- Existence of the file should be known for it to be accessed.
- Data Sharing is not effective as it does not reach every peer.

IV. PROPOSED SYSTEM

The Proposed System implements a peer-to-peer application. This application allows the participating peers to share their data with any other peer in the network. Like the existing system here a data is shared between the peers using request send/receive process. Additionally a peer having a file can share it with another peer using the process of recommendations. A file which is universal in its benefits can be shared between all the peers. So the peer having the file can send a Recommendation to the other peers. Depending on their requirement the recipient peer uses the file.

Advantages:

- Data Sharing is effective in such a peer-to-peer System.
- The data is also shared among trusted peers, thereby maintain security.

V. BLOCK DIAGRAM

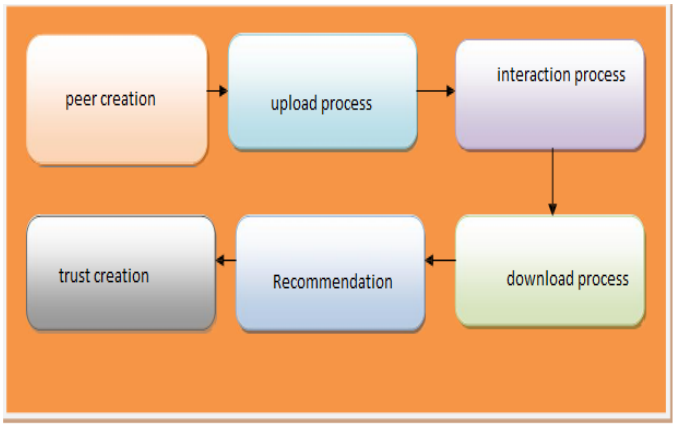


Figure 2. Block Diagram

VI. IMPLEMENNTATION

A. *Peer Creation*

In this module, we create three peers. In SORT, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, e.g., uploading a file. If a peer has no acquaintance, it chooses to trust strangers. An acquaintance is always preferred over a stranger if they are equally trustworthy. We implemented a P2P file sharing simulation tool and conducted experiments to understand impact of this work.

B. *Upload Process*

In this module, we design each peer can upload file and its updated to all the peers. The details of each file with their file name, up-loader name with their IP address are stored continuously. So the peer which needs the file can download it.

C. *Interaction Process*

In this module, we create the interaction process between each peers. The peer which wants the file cannot download it without requesting permission from the uploaded. The peer will request to the uploader with the full details, such as filename etc. The request will be received to the uploader and then its processes.

If the uploader sends the file, then only the peer can download it. With the uploader permission, the peer cannot download it. In this way the peer interaction process module takes place.

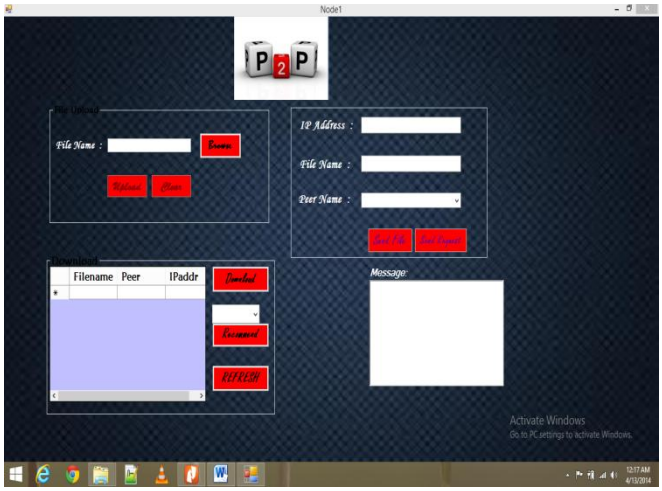
D. *Recommanded Model*

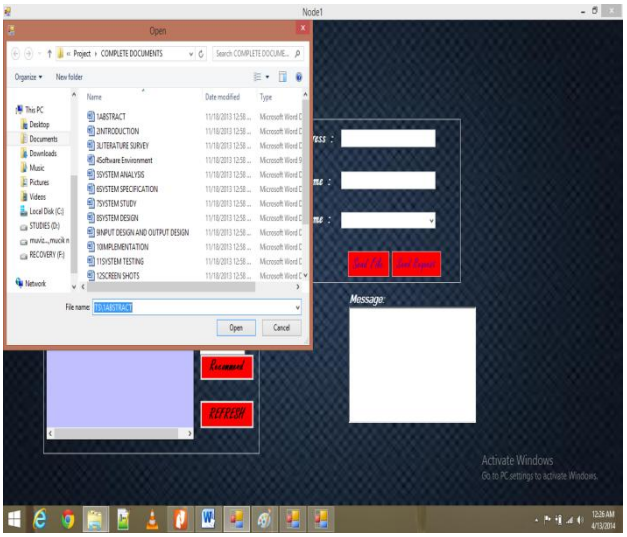
In this module, the recommendation is made to the other peers regarding the service or uploader. A peer may be a good service provider but a bad recommender or vice versa. Thus, the work considers providing services and giving recommendations as different tasks and defines two contexts of trust: service and recommendation contexts. Information about past interactions and recommendations are stored in separate histories to assess competence and integrity of acquaintances in these contexts.

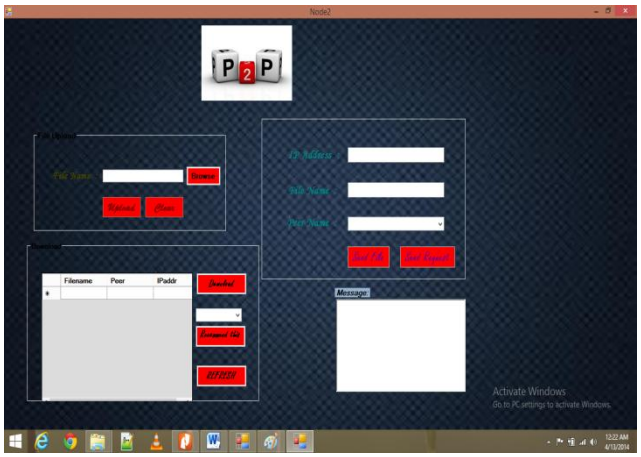
Using a service of a peer is an interaction, which is evaluated based on weight (importance) and recentness of the interaction, and satisfaction of the requester. An acquaintance's feedback about a peer, recommendation, is

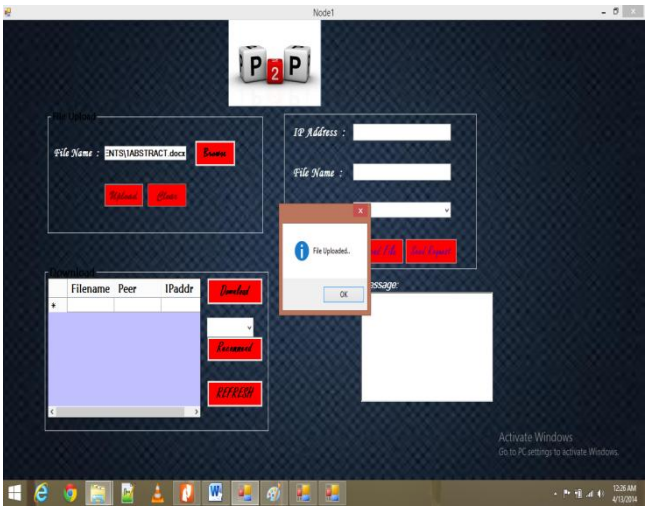
evaluated based on recommender's trustworthiness. It contains the recommender's own experience about the peer, information collected from the recommender's acquaintances, and the recommender's level of confidence in the recommendation.

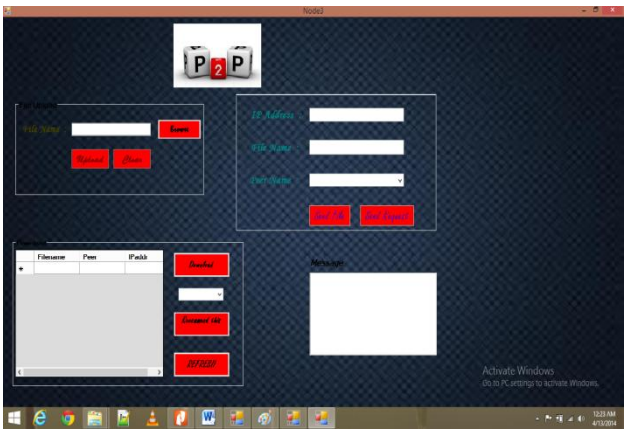
VII. RESULTS

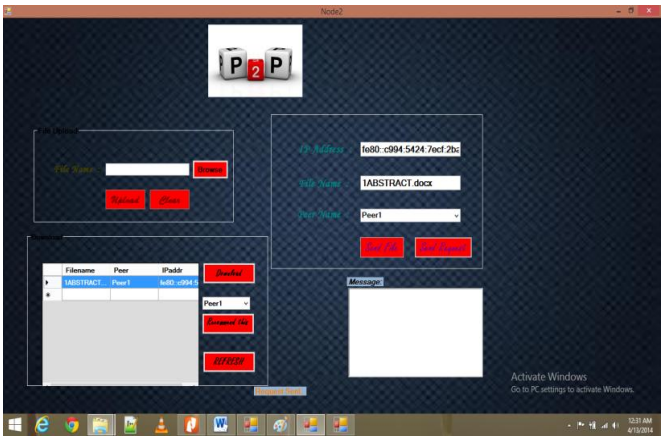


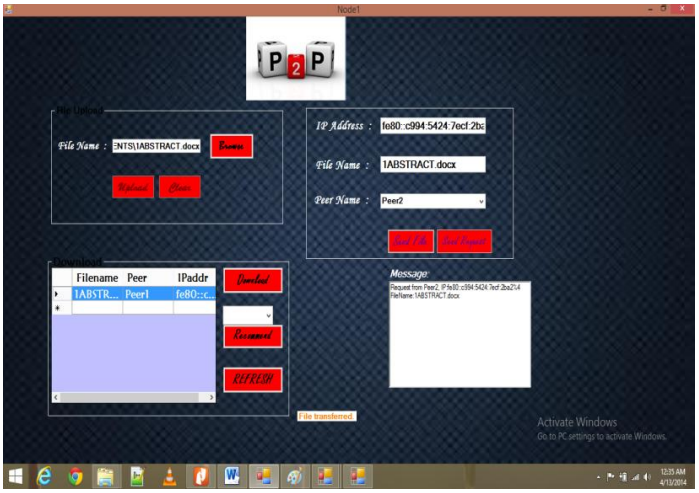


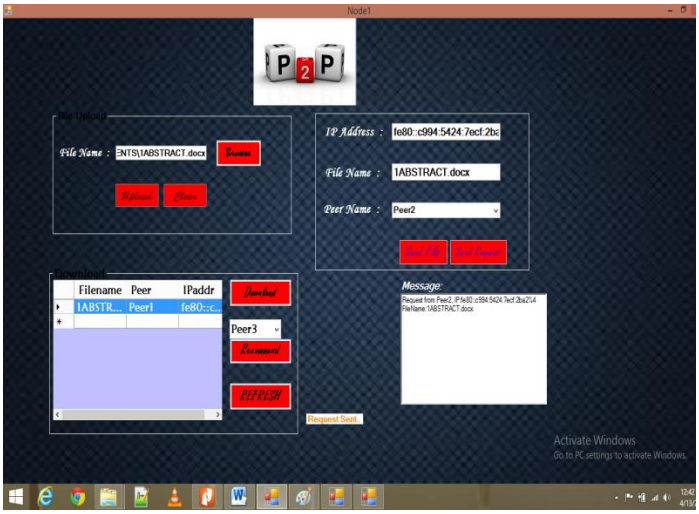


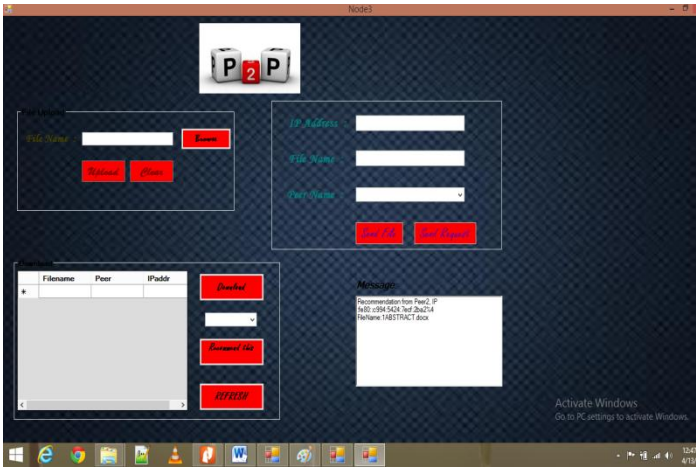












VIII. CONCLUSION

A trust model for P2P networks is presented, in which a peer can develop a trust network in its proximity. A peer can isolate malicious peers around itself as it develops trust relationships with good peers. Two context of trust, service and recommendation contexts are defined to measure capabilities of peers in providing services and giving recommendations. Interactions and recommendations are considered with satisfaction, weight, and fading effect parameters. A recommendation contains the recommender's own experience, information from its acquaintances, and level of confidence in the recommendation. These parameters provided us a better assessment of trustworthiness. Individual, collaborative, and pseudonym changing attackers are studied in the experiments. Damage of collaboration and pseudo spoofing is dependent to attack behavior. Although recommendations are important in hypocritical and oscillatory attackers, pseudospoofers, and collaborators, they are less useful in naive and discriminatory attackers. This work mitigated both service and recommendation-based attacks in most experiments.

However, in extremely malicious environments such as a 50 percent malicious network, collaborators can continue to disseminate large amount of misleading recommendations. Another issue about this work is maintaining trust all over the network. If a peer changes its point of attachment to the network, it might lose a part of its trust network. These issues might be studied as a future work to extend the trust model. Using trust information does not solve all security problems in P2P systems but can enhance security and effectiveness of systems. If interactions are modeled correctly, this work can be adapted to various P2P applications, e.g., CPU sharing, storage networks, and P2P gaming. Defining application specific context of trust and related metrics can help to assess trustworthiness in various tasks.

REFERENCES

[1] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer InformationSystem," Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM),2001.

[2] F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a P2P Network," Proc. 11th World Wide Web Conf. (WWW), 2002.

[3] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in P2P Networks," Proc. 12th World Wide Web Conf. (WWW), 2003.

[4] L. Xiong and L. Liu, "Peertrust: Supporting Reputation-Based Trust for Peer- to-Peer Ecommerce Communities," IEEE Trans. Knowledge and Data Eng., vol.16

[5] A.A. Selcuk, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," Proc. IEEE/ACM Fourth Int'l Symp.Cluster Computing and the Grid (CCGRID), 2004.

[6] R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Networks," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.